CLAIM LISTING

This listing of claims will replace all prior versions, and listings of claims in the application:

In the Claims

Please cancel claim 7 without prejudice.

1.(original) A PLD with decryption and structure for preventing design relocation comprising:

a decryptor for decrypting an encrypted bitstream;

an address indicator for indicating an address into which configuration data will be loaded; and

a decryption algorithm implemented by the decryptor, wherein the decryption algorithm uses data from the address indicator for decrypting the encrypted bitstream.

2.(original) The PLD of Claim 1 wherein the address indicator is an initial address indicator.

3.(original) The PLD of Claim 2 wherein the initial address indicator is a frame address for indicating a starting frame of the PLD into which configuration data will be loaded.

4.(original) The PLD of Claim 1 wherein the decryption algorithm comprises the DES algorithm.

5.(original) The PLD of Claim 4 wherein the DES algorithm includes a cipher block chaining algorithm and the address indicator is placed into a starter value of the cipher block chaining algorithm.

6.(original) The PLD of Claim 4 wherein the DES algorithm includes a cipher feedback mode algorithm and the address indicator is placed into a starter value of the cipher block chaining algorithm.

7.(canceled)

8.(original) The PLD of Claim 1 wherein the address indicator is loaded with a value in the bitstream.

9.(original) The PLD of Claim 8 wherein the value in the bitstream is encrypted.

10.(original) The PLD of Claim 8 wherein the value in the bitstream is not encrypted.

11. (new) A method for configuring a programmable logic device (PLD), comprising:

storing a plurality of decryption keys in storage elements of the PLD;

receiving a configuration bitstream at the PLD, wherein the configuration bitstream includes control data and configuration data, the control data includes an address that references configuration memory of the PLD, and at least the configuration data is encrypted;

decrypting the configuration bitstream in the PLD using the address from the configuration bitstream and the plurality of decryption keys, whereby a decrypted configuration bitstream is generated; and

storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD.

12. (new) The method of claim 11 wherein the address in the configuration bitstream indicates an initial address in configuration memory at which configuration data is to be stored.

13. (new) The method of claim 11, wherein the decrypting step includes performing DES decryption.

14. (new) The method of claim 13, wherein the decrypting step further includes performing DES decryption using cipher block chaining and including the address in an input starter value to the cipher block chaining.

15. (new) The method of claim 13, wherein the decrypting step further includes performing DES decryption using cipher feedback and including the address in an input value to the cipher feedback.

16. (new) The method of claim 11, wherein the address in the bitstream is encrypted.

17. (new) The method of claim 11, wherein the address in the bitstream is not encrypted.

18. (new) The method of claim 11, further comprising disabling readback of configuration data from the PLD after storing the configuration data in configuration memory.

19. (new) The method of claim 18, further comprising disabling partial reconfiguration of the PLD in response to decryption of the configuration bitstream.

20. (new) An apparatus for configuring a programmable logic device (PLD), comprising:

means for storing a plurality of decryption keys in storage elements of the PLD;

means for receiving a configuration bitstream at the PLD, wherein the configuration bitstream includes control data and configuration data, the control data includes an address that references configuration memory of the PLD, and at least the configuration data is encrypted;

means for decrypting the configuration bitstream in the PLD using the address from the configuration bitstream and the plurality of decryption keys, whereby a decrypted configuration bitstream is generated; and

means for storing configuration data from the decrypted configuration bitstream in configuration memory of the PLD.

21. (new) A programmable logic device (PLD), comprising:

a configuration memory;

programmable logic circuitry coupled to the configuration memory;

a key management circuit adapted for storage of a plurality of keys;

a configuration circuit coupled to the configuration memory and to the plurality of storage elements, the configuration circuit adapted to configure the configuration memory with an input configuration bitstream, wherein the configuration bitstream includes control data and configuration data, the control data includes an address that references configuration memory of the PLD, and at least the configuration data is encrypted; and

a decryptor coupled to the configuration circuit and to the plurality of storage elements, the decryptor configured to decrypt, responsive to the configuration circuit, an input configuration bitstream using the address from the configuration bitstream and a plurality of decryption keys stored in the plurality of storage elements.

22. (new) The PLD of claim 21 wherein the address in the configuration bitstream indicates an initial address in configuration memory at which configuration data is to be stored.

23. (new) The PLD of claim 21, wherein the decryptor is adapted to perform DES decryption.

24. (new) The PLD of claim 23, wherein the decryptor is further adapted to perform DES decryption using cipher block chaining and include the address in an input starter value to the cipher block chaining.

25. (new) The PLD of claim 23, wherein the decryptor is further adapted to perform DES decryption using cipher feedback and include the address in an input value to the cipher feedback.

26. (new) The PLD of claim 21, wherein the address in the bitstream is encrypted.

27. (new) The PLD of claim 21, wherein the address in the bitstream is not encrypted.

28. (new) The PLD of claim 21, wherein the configuration circuit is further adapted to disable partial reconfiguration of the PLD and disable readback of configuration data from the PLD responsive to input of an encrypted configuration bitstream, decryption of the encrypted configuration bitstream, and configuration with the decrypted configuration bitstream.